DEPARTMENT OF HOMELAND SECURITY

[Docket No. ICEB-2020-0008]

Privacy Act of 1974; System of Records

AGENCY: U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security.

ACTION: Notice of a New Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the U.S. Department of Homeland Security (DHS) proposes to consolidate two current systems of records, "DHS/U.S. Immigration and Customs Enforcement (ICE)-005 Trade Transparency Analysis and Research System of Records" and "DHS/ICE-016 FALCON Search and Analysis System of Records," into an overarching system of records titled, "DHS/ICE-018 Analytical Records." This new agency-wide system of records notice covers records maintained by ICE to allow personnel to search, aggregate, and visualize large volumes of information to enforce criminal, civil, and administrative laws under ICE's jurisdiction. Additionally, DHS is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act elsewhere in the Federal Register. This newly established system will be included in the Department's inventory of record systems.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This modified system will be effective upon publication. Routine uses will be effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number ICEB-2020-0008 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: James Holzer, Acting Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number ICEB-2020-0008. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Jordan Holz, ICEPrivacy @ice.dhs.gov, Privacy Officer, U.S. Immigration and Customs Enforcement (ICE), 500 12th Street SW, Mail Stop 5004, Washington, D.C. 20536. For privacy questions, please contact: James Holzer, (202) 343-1717, Privacy@hq.dhs.gov, Acting Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

The U.S. Department of Homeland Security (DHS)/U.S. Immigration and Customs Enforcement (ICE) proposes to issue a new DHS system of records notice (SORN) titled, "DHS/ICE-018 Analytical Records." DHS/ICE is creating this new system of records to better reflect and clarify the nature of all records collected, maintained, processed, and shared by ICE in large analytical data environments.

This system of records consolidates the following two notices, "DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) System of Records," 79 Fed. Reg. 71112 (December 1, 2014), and "DHS/ICE-016 FALCON Search and Analysis

(FALCON-SA) System of Records," 82 Fed. Reg. 20905 (May 4, 2017), into one new system of records. This new system of records reflects the types of information and records ICE collects and maintains in analytical systems to support its law enforcement and investigative mission, rather than linking the SORN to specific IT system(s). This SORN provides greater transparency of ICE's processes and more accurately reflects the storage of records in the cloud computing environment. After the routine uses of this SORN are effective, ICE will publish a rescindment notice for both the DHS/ICE-005 TTAR SORN and the DHS/ICE-016 FALCON-SA SORN.

ICE analytical systems help ICE personnel conduct research and analysis using advanced analytic tools in support of their law enforcement and investigative mission. These tools allow ICE to query, analyze, and present large amounts of data in a variety of formats that can help illuminate relationships among the various data elements. Some analytical tools may incorporate the use of artificial intelligence and machine learning to assist ICE personnel in examining large and complex datasets. All analytical systems and tools under this system of records use a central data store to eliminate the need for multiple copies of the data. The central data store streamlines the application of many security and privacy controls. Source systems control user access, retention, and dissemination restrictions on the record level by data tagging. Data tagging is the process of indexing or labeling data individually, instead of only labelling data at the system or folder level. Records covered by this SORN may reside physically within the same platform or cloud computing environment, but are logically separated from each other through the data tagging process. ICE personnel would therefore only have access to the information for which they have a pre-established need to know.

Strong access controls and robust audit functions within the analytical systems ensure that ICE's use of the records is predicated on law enforcement, national security, immigration enforcement, and customs enforcement activities. A governance group

composed of leadership from ICE Homeland Security Investigations (HSI) enforces this requirement, with oversight by ICE's legal and privacy offices.

Data derived from other SORNs

This system of records ingests and aggregates data from a number of system and database interfaces that collect data for ICE's law enforcement, national security, immigration enforcement, and customs enforcement missions. ICE controls all data aggregated from these interfaces through a combination of data tagging, access control lists, and other technologies. These interfaces are covered by other federal agency, DHS, and ICE SORNs. Separate SORNs are appropriate because the data, purposes, and routine uses differ depending on the analytical interface or tool. ICE ensures that the appropriate retention, use, and sharing of this data is in line with the purpose of its original collection. Records available to users via other system interfaces are covered by these separate SORNs, which are customized to the purposes of those interfaces. For example, data available through an ingest from ICE's Investigative Case Management System (ICM) interface would be covered by the DHS/ICE-009 External Investigations SORN, 75 Fed. Reg. 404 (January 5, 2010).

The analytical data store ingests information either on a routine or ad hoc basis. Routine ingests are regular updates to datasets that originate from other government (typically ICE or DHS) data systems. Ad hoc ingests are user-driven ingests of particular data that may be relevant to a given user or group's investigative or analytical project in the analytical system. The nature of the data in ad hoc ingests varies. For example, data may be collected from commercial or public sources (e.g., internet research or from a commercial data service), public reports of law enforcement violations or suspicious activity (tips), or digital records seized or subpoenaed during an investigation. Data uploaded to analytical systems in an ad hoc manner is associated with a case file number, if possible, and retained consistent with the retention of the case file. ICE collects data for

ad hoc ingests in accordance with the purposes outlined in an ICE or DHS SORN and will tag the record with the appropriate category description. That tag controls the use, dissemination, and retention policy for that data.

Stand-Alone Analytical Records

The analytical data store also contains metadata that is created by an ICE analytical system when it ingests data. ICE uses the metadata to apply access controls and other system rules (such as retention policies) to the contents of the central data store. The metadata also provides important contextual information about the date the information was added to the data store and the source system where the data originated.

Analytical systems covered by this SORN may also contain an index, which is a numerical and alphabetical list of every word or string of numbers/characters found in the system, with a reference to the electronic location where the corresponding source record is stored. Analytical systems use indexes to conduct searches, identify relationships and links between records and data, and generate visualizations for analytic purposes.

ICE analytical systems also ingest external information from non-federal entities, including state and local law enforcement authorities, private corporations, or foreign governments. External information shared with ICE could include any category of records listed in this SORN, such as biographic information, trade and customs information, criminal history information, content from the dark net, and publicly available social media content. ICE determines the parameters on retention, use, and sharing of the information via an agreement between the entity and ICE, such as a memorandum of understanding or ICE agreeing to the terms and conditions of a private service. Like ad hoc ingests, ICE collects information from non-federal entities in accordance with the purposes outlined in an ICE or DHS SORN and will tag the record with the appropriate category description. ICE may use external entity ingests for law

enforcement, national security, immigration enforcement, and customs enforcement purposes.

This SORN also covers tips submitted to ICE via email, online forms on the ICE website, or by calling an ICE tip line phone number. These tips are created electronically using an ICE-wide tip line interface or may be manually entered by ICE analysts. The tips are input directly into ICE analytical systems and are vetted using analytical tools. Once ICE analysts adjudicate the tips for action, the tips will then be referred via the analytical system to the relevant ICE office or program and accessible to authorized users to conduct further investigation.

Users of an analytical tool or system may create visualizations, match records, or create analyses of large volumes of data through algorithmic processes. The end result of user efforts with an analytical tool, such as a map or list, is an analytical work product. Work products are considered intermediary records with access, use, and sharing restrictions tied to the underlying raw data that a system used to create the product. Analytical work products are destroyed upon verification of successful creation of the final document or file or when no longer needed for a business use, whichever is later. If a user deems the product to be pertinent to an investigation, it will then be incorporated into a final document or file as an investigative record and follow the case with which it was assigned.

Analytical products, information sharing, and user collaboration made possible in analytical systems may result in the creation of a lead to the field. These leads are actionable intelligence that require further investigation by ICE prior to agents or officers carrying out any law enforcement action. Analytical systems may distribute and track the outcomes of leads for reporting purposes.

Finally, as this SORN will replace the DHS/ICE-005 TTAR SORN, it will now provide notice for use of all data collected by ICE that is used in generating leads for, and

otherwise supporting, investigations related to customs violations. These violations include trade-based money laundering, smuggling, commercial fraud, and other crimes within the jurisdiction of ICE. For example, ICE uses financial and law enforcement data to examine foreign trade data to identify anomalies in patterns of trade. Such anomalies can indicate import-export crimes that ICE is responsible for investigating. In addition, these anomalies, patterns, and relationships provide leads that may warrant investigation for violation of U.S. export laws and regulations.

Uses of data within the system

ICE agents and criminal analysts use analytical systems for a variety of purposes: to conduct research that supports the production of law enforcement intelligence products; to provide lead information for investigative inquiry and follow-up; to support the enforcement and investigation of criminal and civil laws under ICE's jurisdiction, including those pertaining to customs violations; to identify potential criminal activity, immigration violations, and threats to homeland security; to share analytical capabilities within DHS and with domestic and foreign partners, as appropriate; to assist in the disruption of terrorist or other criminal activity; and to discover previously unknown connections among existing ICE investigations.

Consistent with DHS's information sharing mission, information stored in the DHS/ICE-018 Analytical Records system of records may be shared with other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/ICE may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

Additionally, DHS is issuing a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act elsewhere in the Federal

Register. This newly established system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which federal government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/ICE-018 Analytical Records system of records.

In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER: U.S. Department of Homeland Security (DHS)/Immigration and Customs Enforcement (ICE)-018 Analytical Records.

SECURITY CLASSIFICATION: Classified, Unclassified, Law Enforcement Sensitive, and For Official Use Only.

SYSTEM LOCATION: Records are maintained either at the ICE Headquarters in Washington, D.C. and field offices, or designated cloud computing environments.

SYSTEM MANAGER(S): Assistant Director for Homeland Security Investigations Operational Technology and Cyber Division, HSIOTCDTasking@ice.dhs.gov, U.S. Immigration and Customs Enforcement, 500 12th Street SW, Washington, D.C. 20536.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 6 U.S.C. sec. 236; 8 U.S.C. secs. 1103 and 1105; 8 U.S.C. secs. 1225(d)(3) and (d)(4)(A); 8 U.S.C. sec. 1324a(e)(2)(C); 8 U.S.C. sec. 1357; 8 U.S.C. sec. 1360(b); 18 U.S.C. secs. 541, 542, 545, and 554; 18 U.S.C. secs. 1956, 1957, and 1960; 18 U.S.C. sec. 2703; 19 U.S.C. sec. 1415; 19 U.S.C. secs. 1481 and 1484; 19 U.S.C. sec. 1509; 19 U.S.C. sec. 1589a; 19 U.S.C. sec. 1628; 19 CFR 161.2 and 192.14; 21 U.S.C. sec. 967; 22 U.S.C. sec. 2778; 31 U.S.C. sec. 5316; 31 CFR 1010.340; 50 U.S.C. sec. 1705; 50 U.S.C. sec. 2411(a); and, Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114-24 (1970).

PURPOSE(S) OF THE SYSTEM: The purposes of ICE analytical systems are:

(a) to support ICE's collection, analysis, reporting, and distribution of law enforcement, customs, immigration, terrorism, intelligence, and homeland security information in support of ICE's mission;

(b) to produce investigative leads and other actionable information to ICE's law enforcement, customs, and immigration enforcement personnel and to other appropriate government agencies;

(c) to identify potential violations of U.S. criminal, civil, and administrative laws through search, aggregation, analysis, and visualization of raw data;

(d) to enhance the efficiency and effectiveness of the research and analysis process for DHS law enforcement, customs, immigration, and intelligence personnel through information technology tools that provide for advanced search and analysis of various datasets;

(e) to facilitate multi-jurisdictional cooperation and collaboration on investigations into transnational activities that violate criminal and civil laws pertaining

to exportation of restricted materials, cargo safety and security, immigration, trafficking, trade, financial crimes, smuggling, and fraud;

(f) to support the operation of the agency's tip line and the collection, analysis, and action on information volunteered by the public and other sources concerning suspicious and potentially illegal activity; and

(g) to identify potential criminal activity, immigration violations, customs violations, and threats to homeland security; to uphold and enforce the law; and to ensure public safety.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Categories of individuals covered by this system include:

(1) individuals identified in law enforcement, intelligence, crime, and incident reports (including financial reports under the Bank Secrecy Act and law enforcement bulletins) produced by DHS and other government agencies;

(2) individuals identified in U.S. passport, visa, border, immigration, and naturalization benefit data, including arrival and departure data;

(3) individuals identified in DHS law enforcement, licensing, and immigration records, including records associated with the ICE Student Exchange Visitor Program;

(4) individuals who, as importers, exporters, shippers, transporters, customs brokers, owners, purchasers, manufacturers, consignees, or agents thereof, participate in the import or export of goods to or from the United States or to or from nations with which the United States has entered an agreement to share trade information;

(5) individuals (e.g., subjects, witnesses, associates, assigned government personnel) associated with customs enforcement, immigration enforcement, administrative actions, detainer requests, or law enforcement investigations/activities conducted by ICE, the former Immigration and Naturalization Service (INS), U.S. Customs and Border Protection (CBP), or the former U.S. Customs Service;

(6) individuals associated with law enforcement investigations or activities conducted by other federal, state, tribal, territorial, local or foreign agencies where there is a potential nexus to ICE's law enforcement, customs enforcement, and immigration enforcement responsibilities, or homeland security in general;

(7) individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism;

(8) individuals involved in or associated with suspicious activities, threats, or other incidents reported by domestic and foreign government agencies, multinational or non-governmental organizations, critical infrastructure owners and operators, private sector entities and organizations, and individuals;

(9) individuals who are subjects of government screening lists or threat assessments, such as known or suspected Transnational Organized Criminal (TOC) gang members or associates;

(10) Specially Designated Nationals (SDN) as defined by 31 CFR 500.306 and individuals identified on other denied parties or screening lists; and

(11) ICE personnel or personnel from partner law enforcement agencies who are mentioned in significant incident reports that concern law enforcement operations, injuries to law enforcement personnel, or other significant incidents reported within ICE.

CATEGORIES OF RECORDS IN THE SYSTEM:

(1) Biographic and other identifying information, including names; dates of birth; places of birth; Social Security numbers (SSN); Tax Identification Numbers (TIN); Exporter Identification Numbers (EIN); passport information (number and country of issuance); citizenship; nationality; location and contact information (e.g., home, business, and email addresses and telephone numbers); and other identification numbers (e.g., Alien Registration Number (A-number), Driver's License Number);

(2) Biometric information, including facial images, iris images, fingerprints,

and voice audio; and any unique numerical identifiers assigned to biometrics for administrative purposes;

(3) Financial data, including data reported pursuant to the Bank Secrecy Act (e.g., certain transactions over $10,000) and other financial data obtained via official investigations, legal processes, or legal settlements. Financial data includes bank account numbers, transaction numbers, and descriptions or value of financial transactions;

(4) Licensing information related to applications by individuals or businesses to hold or retain a customs broker's license, operate a customs-bonded warehouse, or be a bonded carrier or bonded cartman;

(5) Trade analysis data, including trade identifier numbers (e.g., for manufacturers importers, exporters, and customs brokers) and bill of lading data (e.g., consignee names and addresses, shipper names and addresses, container numbers, carriers); internet protocol (IP) addresses; other financial data related to trade required for the detection and analysis of financial irregularities and crimes;

(6) Location-related data, including address; geotags from metadata associated with other record categories collected; and geolocation information derived from authorized law enforcement activities, ICE-owned devices, witness accounts, or commercially available data;

(7) Various internal operational reports, including reports of significant incidents and operations; reports concerning prospective enforcement activity; reports of outcomes and dispositions of referred leads; requests for assistance from other law enforcement agencies; agency intelligence reports; and reports of third-agency visits to ICE detention facilities;

(8) Law enforcement records, including TECS subject records and investigative records related to an ICE or CBP law enforcement matter, information obtained from the U.S. Department of the Treasury's Specially Designated Nationals List, visa security

information, and other trade-based and financial sanction screening lists. Law enforcement data includes names; aliases; business names; addresses; IP addresses; dates of birth; places of birth; citizenship; nationality; passport information; SSNs; TINs; Driver's License Numbers; and vehicle, vessel, and aircraft information;

(9) Reports of fines, penalties, forfeitures, and seizure incidents;

(10) Financial and communication records obtained during the course of an ICE criminal investigation. These records can include lawfully obtained call transactions, call content, text transactions, text content, email transactions, email content, and financial wire transactions;

(11) Continued presence parole application records;

(12) Open source information - news articles or other data available to the public on the internet or in public records, including content from the dark net and publicly available information from social media;

(13) Commercially available data - public and proprietary records available for a subscription;

(14) Cargo and border crossing data – inbound/outbound shipment records and border crossing information;

(15) Criminal information, including lookouts, warrants, criminal history records, and other civil or criminal investigative information provided by other law enforcement agencies;

(16) Information from foreign governments or multinational organizations such as INTERPOL or Europol – including criminal history; immigration data; passenger, vehicle, vessel entry/exit data; passport information; vehicle, vessel, and licensing records; shipment records; telephone records; intelligence reports; investigative leads and requests; and wanted persons notices, warrants, and lookouts;

(17) Information related to participation in a student exchange visitor program,

including education and training; school information; sponsor information; program status and activities; placement information; and any administrative or adjudicative actions related to the program;

(18) Investigative leads, analytical work products, and finished intelligence reports from ICE, DHS, or other agencies;

(19) Information or evidence seized or otherwise lawfully obtained during the course of an ICE investigation, including business records, third-agency records, public records (e.g., courts), transcripts of interviews/depositions, or records and materials seized or obtained via subpoena or other lawful process;

(20) Tips concerning illegal or suspicious activity from the public and other law enforcement agencies; and

(21) Tip data concerning child exploitation violations, such as the biographical data of the suspect or the suspect's online identity information (e.g., user ID). Internet service provider data, domain name, credit card number and IP address, internet subscriber data (e.g., name, subscriber number, billing address, payment method, and email addresses), a log of subscriber activity, or other information such as motor vehicle data, and SSN; and

(22) Other information collected during the course of vetting a tip from sources such as government databases, open sources, and commercially-available data, as previously described.

RECORD SOURCE CATEGORIES: Records are obtained from individuals via tips to the ICE tip line or other public interfaces; other DHS components; U.S. Department of Commerce; U.S. Department of the Treasury; U.S. Department of State; other federal, state, and local law enforcement agencies; foreign governments pursuant to international agreements or arrangements; international entities; financial institutions; transportation companies; manufacturers; customs brokers; organizations participating in free trade

zones; port authorities; and commercially and publicly available data sources. Current federal interfaces with ICE analytical systems include records covered by the following SORNs:

- DHS/ICE-001 Student Exchange Visitor Information System (SEVIS), 75 FR 412 (January 5, 2010);
- DHS/ICE-004 Bond Management Information System (BMIS), 85 Fed. Reg. 64515 (October 13, 2020);
- DHS/ICE-006 Intelligence Records System (IIRS), 75 Fed. Reg. 9233 (March 1, 2010);
- DHS/ICE-007 Criminal History and Immigration Verification (CHIVe) System of Records, 83 Fed. Reg. 20844 (May 8, 2018);
- DHS/ICE-008 Search Arrest and Seizure Records, 73 Fed. Reg. 74732 (December 9, 2008);
- DHS/ICE-009 External Investigations, 75 Fed. Reg. 404 (January 5, 2010);
- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 Fed. Reg. 72080 (October 19, 2016);
- FinCEN .003 - Bank Secrecy Act Reports System, 79 Fed. Reg. 20969 (April 14, 2014);
- DHS/CBP-006 Automated Targeting System, 77 Fed. Reg. 30297 (May 22, 2012);
- DHS/CBP-020 Export Information System, 80 Fed. Reg. 53181 (September 2, 2015);
- JUSTICE/FBI-001 National Crime Information Center (NCIC), 84 Fed. Reg. 47533 (September 10, 2019);
- DHS/ALL-041 External Biometric Records (EBR), 83 Fed. Reg. 17829 (April 24, 2018).

SORNs ingested into analytical systems at ICE are subject to change based on mission need and requirements of both ICE and system owners.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. sec. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including the U.S. Attorneys Offices, or other federal agencies conducting litigation or proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity, only when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. secs. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another federal agency or federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

I. To federal, state, local, tribal, territorial, foreign or international agencies, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual; the issuance, grant, renewal, suspension, or revocation of a security clearance, license, contract, grant, or other benefit; or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security

J. To appropriate federal, state, local, tribal, territorial, or foreign government agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty when DHS determines that the information would assist in the enforcement of civil, criminal, or regulatory laws.

K. To federal, state, local, tribal, territorial, foreign government agencies, or other entities or individuals, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of national security, intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, executive order, or other applicable national security directive.

L. To federal, state, local, tribal, territorial, or foreign government agencies or organizations, or international organizations, lawfully engaged in collecting law enforcement intelligence, whether civil or criminal, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

M. To international, foreign, intergovernmental, and multinational government agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.

N. To a court, magistrate, administrative tribunal, opposing counsel, parties, and witnesses in the course of a civil, criminal or administrative proceeding before a court or adjudicative body when DHS determines that the use of such records is relevant and necessary to the litigation or the proceeding provided that in each case, DHS determines that disclosure of the information to the recipient is a use of the information that is compatible with the purpose for which it was collected.

O. To federal, state, local, tribal, territorial, or foreign government agencies, as well as to other individuals and organizations during the course of an investigation by DHS or the processing of a matter under DHS's jurisdiction, or during a proceeding within the purview of the immigration and nationality laws, when DHS deems that such disclosure is necessary to carry out its functions and statutory mandates or to elicit information required by DHS to carry out its functions and statutory mandates.

P. To federal, state, local, tribal, territorial, international, or foreign government agencies or entities for the purpose of consulting with those agencies or entities:

(1) To assist in making a determination regarding redress for an individual in connection with the operations of a DHS component or program;

(2) To verify the identity of an individual seeking redress in connection with the operations of a DHS component or program; or to verify the accuracy of information submitted by an individual who has requested redress on behalf of another individual.

Q. To an organization or individual in either the public or private sector, either foreign or domestic, to the extent necessary to prevent immediate loss of life, serious bodily injury, or destruction of property.

R. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure

is appropriate to the proper performance of the official duties of the officer making the disclosure.

S. To a former employee of DHS for the purpose of responding to an official inquiry by federal, state, local, tribal, or territorial government agencies or professional licensing authorities; or facilitating communications with a former employee that may be necessary for personnel-related matters or other official purposes when DHS requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

T. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to use relevant data, that relate to the purpose(s) stated in this SORN, for purposes of testing new technology.

U. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS/ICE stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media within secure access-controlled facilities.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: DHS/ICE may retrieve records by any of the personal identifiers stored in the system including name, business address, home address, importer ID, exporter ID, broker ID, manufacturer ID,

Social Security number, trade and tax identifying numbers, passport number, or account number. Records may also be retrieved by non-personal information such as transaction date, entity or institution name, description of goods, value of transactions, and other information.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: The retention period for information contained in analytical systems varies depending on the type of data. Routinely ingested data is retained in accordance with the record retention schedule of the source system. Analytical products are considered intermediary records which are destroyed upon verification of successful creation of the final document or file (such as a generated lead), or when no longer needed for a business use, whichever is later. Data uploaded to analytical systems in an ad hoc manner is associated with a case file number, to the extent possible, and retained consistent with the retention of the case file. Records associated with an ICE case file, either ad hoc uploads or designated analytical work products, are active until the case closes, and then will be retained for 20 years in accordance with legacy customs schedule N1-36-86-1-161.3 (inv 7B) from the Department of Treasury. Records associated with cases are retained for evidentiary purposes, to allow ICE to link findings to other cases, and to ensure ICE has proper auditing and oversight of its systems. ICE will develop and submit an updated schedule for investigative records to the National Archives and Records Administration (NARA) for approval. When there is no case file number, ICE tags the data as either associated with the ICE or DHS SORN related to the original collection of the information or with a retention schedule of 20 years. ICE retains system metadata for the same length of time as the record or data element they originate from or describe.

Currently, the retention period for data maintained under the DHS/ICE-005 TTAR SORN is maintained in accordance with the legacy retention schedule N1-567-09-003. Case related records under this schedule will remain active until the end of the

calendar year in which a case closes, after which it will be retainedfor an additional ten years, and then deleted. All other bulk financial and trade data ingested is archived at the end of the calendar year of receipt and destroyed three years thereafter. ICE intends to request NARA approval to retire the legacy retention schedule and proposes to retain all financial and trade data for ten years.

This system of records will also be the official repository for tip information at ICE. The tip line application will feed records it creates directly into an analytical central storage environment. ICE analysts may manually enter other tip information into the environment. Currently tip records are unscheduled. ICE will include tip records in its submission to NARA for a new investigative records schedule. ICE will propose that standard tip records be retained for ten years from the date of the tip. Tip records concerning child exploitation crimes will be retained for 75 years in line with retention schedule N1-567-10-014.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS/ICE safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS/ICE has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES: The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and the Judicial Redress Act if applicable, because it is a law enforcement system. However, DHS/ICE will consider individual requests to determine whether or not information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a

request in writing to the Chief Privacy Officer and ICE Freedom of Information Act (FOIA) Officer whose contact information can be found at http://www.dhs.gov/foia under "Contact Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, U.S. Department of Homeland Security, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about an individual may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, the individual should:

- Explain why he or she believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believes may have the information;
- Specify when the individual believes the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If the request is seeking records pertaining to another living individual, the request must include an authorization from the individual whose record is being requested, authorizing the release to the requester.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act or covered JRA records, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record.

NOTIFICATION PROCEDURES: See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); (f); and (g). Pursuant to 5 U.S.C. 552a(k)(2), this system is exempt from the following provisions of the Privacy Act, subject to the limitations set forth in those subsections: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H); and (f). When an analytical system receives a record from another system exempted in that source system under 5 U.S.C. sec. 552a(j)(2), ICE will claim the same

exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

HISTORY: DHS/ICE-005 Trade Transparency Analysis and Research, 79 Fed. Reg. 71112 (December 1, 2014); DHS/ICE-016 FALCON Search and Analysis, 82 Fed. Reg. 20905 (May 4, 2017).

*****

James Holzer,
Acting Chief Privacy Officer,
U.S. Department of Homeland Security.
[FR Doc. 2021-05651 Filed: 3/19/2021 8:45 am; Publication Date: 3/22/2021]